State of Iowa Enterprise Wireless LAN Standard

July 13, 2006

Purpose

This standard establishes minimum requirements for installation and operation of Wireless Local Area Networks (WLANs) for State of Iowa Agencies. The intent of the standard is to protect the security of State Information Technology (IT) resources.

Overview

Wireless communications may provide agencies and users benefits such as portability and flexibility, increased productivity, and lower installation costs. A wireless local area network (WLAN) is a wireless technology that allows computers to share files and applications without being tethered by a wire. For example, users can move laptops from place to place within their offices without the need for wires and without losing access to e-mail or documents. In many environments, the opportunities to improve service or decrease cost can be substantial.

The benefits of wireless networking, however, come with potential risks. Some risks are similar to those of wired networks; some are exacerbated by wireless connectivity; some are new. A significant source of risk in wireless networks is the technology's underlying communications medium, the airwave, which could result in the logical equivalent of a network port in the parking lot. Unauthorized users or processes may gain access to agency systems and information, corrupt the agency's data, consume network bandwidth, degrade network performance, and launch attacks that prevent authorized users from accessing the network, or use agency resources to launch attacks on other networks.

Scope

This document presents minimum standards which must be met by agencies using wireless local area network technologies. For the purpose of this standard, security is defined as the ability to protect the integrity, confidentiality and availability of information processed, stored and transmitted by an agency and includes protection from unauthorized use or modification and from accidental or intentional damage or destruction. Information technology assets covered by this standard include information technology facilities and off-site data storage, computing, telecommunications and applications related services purchased from other state agencies or commercial entities and Internet-related applications and connectivity.

This standard applies to all agencies as defined by Iowa Code Chapter 8A, Section 101. Non-participating agencies are encouraged to follow the guidelines in this and other enterprise level policies, standards, guidelines, processes and procedures.

Definitions

Selected terms used in the Enterprise WLAN Policy are defined below:

- **Access Point (AP):** A hardware device or a computer's software that acts as a communication hub for users of a wireless device to connect to a wired Local Area Network. APs are important for providing heightened wireless security and for extending the physical range of service to which a wireless user has access.

- **Chief Information Security Officer (CISO):** The person responsible for enterprise information security located in the Department of Administrative Services, Information Security Office.

- **Denial of Service (DoS):** The prevention of authorized access to system assets or services or the delaying of time-critical operations.

- **Local Area Network (LAN):** A network that connects computers in close proximity via cable, usually in the same building.

- **Radio Frequency (RF):** Any frequency within the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that then is able to propagate through space. Many wireless technologies are based on RF field propagation.

- **Service Set Identifier (SSID):** A 32-character unique identifier. The SSID differentiates one WLAN from another; so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. An SSID is essentially the name of the network.

- **Simple Network Management Protocol (SNMP):** An Internet Standard protocol for remotely managing computer network devices. SNMP Version 3 provides enhanced, integrated support for security services, including data confidentiality, data integrity, data origin authentication, and message timeliness and limited replay protection.

- **WLAN (WLAN):** A LAN where devices connect to the network using wireless technology.

Enterprise WLAN Standard

If security controls are not in place or they are configured improperly, the process of establishing WLANs can expose all connected systems to access by unauthorized personnel and malicious

software. Therefore, to ensure that all connections are made properly and securely, the following minimum standards must be met for all WLANs:

1. **Access Point Registration.** An agency shall notify the Chief Information Security Officer at least 5 business days prior to implementation of a wireless local area network. The notification must include, at a minimum, the department name, access point locations, and service set identifier.

2. **Multiple network connections.** Devices connected to the wireless local area network must not be connected to a wired network at the same time, except for firewalls or other packet-filtering devices expressly designed for that purpose.

3. **Separation of wireless and wired networks.** A firewall or other packet-filtering device shall be placed between the wireless access point and the wired network. The device must be configured so that all traffic is blocked except for that which is required to meet business needs.

4. **Critical Devices.** File servers, database servers, application servers and related devices critical to the operation of the agency are not allowed on wireless networks.

5. **Physical protection.** Wireless access points must be placed in a physically protected location that limits opportunity for theft, damage or unauthorized access. Many wireless access points have reset features, which may allow an individual that can touch the access point to clear all agency-established security settings.

6. **Wireless access point configuration.** Agencies shall configure access points in accordance with the following requirements:

    - **Default passwords shall be changed.** Administrators shall change default settings to reflect the requirement for strong (i.e., an alphanumeric and special character string at least eight characters in length) administrative passwords. Two-factor authentication should be considered in addition to strong administrative passwords.

    - **Proper encryption settings shall be established.** Encryption settings must be set for the strongest encryption available in the product. Wired Equivalent Privacy (WEP) must not be used. Wi-Fi Protected Access (WPA) must be used at a minimum.

    - **The Service Set Identifier shall be changed.** The SSID of the AP shall be changed from the factory default setting. The SSID should be long, include numbers and both upper and lower case letters and not include information that indicates the location or purpose of the WLAN.

    - **Beacon intervals shall be maximized.** The 802.11 standard specifies the use of "Beacon frames." These beacons are transmitted from APs at regular intervals and allow a client station to identify and match configuration parameters in order to join a wireless network. Agencies shall set the interval length to its maximum value.

- **SSID broadcast features shall be disabled.** The SSID is used to assign an identifier to the WLAN. By default, the SSID is broadcast so wireless devices can learn the name of the network to make it easier to connect. When the broadcast SSID feature of an AP is disabled the client must supply the correct SSID to connect to the network.

- **Default cryptographic keys shall be changed.** Many manufacturers of APs use the same factory setting for encryption on every AP they produce. If the factory setting is not changed, the encryption can be easily defeated. Agencies shall therefore change default cryptographic keys before implementing a new AP.

- **Shared key authentication.** If shared cryptographic keys are used they shall be changed at least every three months and when there are key personnel changes within the agency.

- **Address filtering:** Media Access Control (MAC) address filtering shall be enabled whenever possible. Only connections from recognized MAC addresses should be accepted by the AP.

- **Simple Network Management Protocol version 3 shall be used if possible.** Some wireless APs use SNMP agents, which allow network management software tools to monitor the status of wireless APs and clients. Agencies that require SNMP must change each default community string to a strong community string, whenever possible. Privileges should be set to "read only" if that is the only access a user requires. Unneeded access ports should be disabled.

- **AP default channels shall be changed.** Vendors commonly use default channels in their APs. If two or more APs are located near each other but are on different networks, a Denial of Service can result from radio interference between the two APs.

7. **Operating logs.** Wireless access points must be set to log operating events including successful and failed login attempts, errors and reboots. The logs should be maintained on a separate file server.

8. **Infrastructure configuration:** The wireless network shall be configured for infrastructure mode. Ad-Hoc mode allowing peer-to-peer communications between wireless devices is not allowed.

9. **Intrusion detection.** An intrusion detection or intrusion prevention system shall be used to detect unauthorized access attempts and inappropriate use of the wireless local area network.

10. **Client security maintained.** All computers connecting to the wireless network must have a properly-configured, host-based firewall, up-to-date antivirus software and be

compliant with applicable enterprise and agency standards. Software patches must be applied per the agency's patching schedule.

11. **Assessment.** The chief information security officer will assess state facilities to determine if unauthorized or improperly configured wireless local area networks are present.

12. **Awareness Training:** Wireless network users shall be provided with wireless security awareness training, including but not limited to documentation describing wireless computing risks.